Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) An authentication method comprising:

generating an initialization vector at a first electronic device;

determining at the first electronic device whether the initialization vector falls within a first group of initialization vectors, the first group including a plurality of initialization vectors solely used in connection with an authentication sequence; and

encrypting information using in part the initialization vector for return to a second electronic device if the initialization vector falls within the first group.

2. (original) The authentication method of claim 1, wherein the first electronic device is a wireless unit.

3. (original) The authentication method of claim 1, wherein the second electronic device is an access point.

4. (original) The authentication method of claim 1, wherein prior to generating the initialization vector, the method comprises receiving the information from the second electronic device by the first electronic device.

5. (original) The authentication method of claim 4, wherein the information is a challenge text.

6. (original) The authentication method of claim 5, wherein the challenge text is a first sequence of bits and the initialization vector is a second sequence of bits produced by a number generator.

7. (original) The authentication method of claim 4, wherein the number generator is a pseudo-random number generator.

8. (original) The authentication method of claim 1 further comprising regenerating an initialization vector if the initialization vector fails to fall within the first group.

9. (original) The authentication method of claim 1, wherein the determining whether the initialization vector falls within the first group includes determining whether a selected series of bits of the initialization vector has been set.

10. (original) The authentication method of claim 9, wherein the selected series of bits is continuous.

11. (original) The authentication method of claim 5, wherein prior to receiving the challenge text, the method further comprises negotiating a shared secret key between the first electronic device and the second electronic device.

12. (original) The authentication method of claim 11, wherein the encrypting of the information includes

combining the initialization vector with the shared secret key; and

repeatedly performing bitwise Exclusive-OR (XOR) operations on the challenge text using a combination of the initialization vector with the shared secret key.

13. (original) The authentication method of claim 5 further comprising:

transmitting both the encrypted challenge text and the initialization vector to the second electronic device;

decrypting the encrypted challenge text using both the initialization vector and a prestored copy of the shared secret key to recover a challenge text; and

comparing the recovered challenge text with the challenge text.

14. (previously presented) A method for authenticating a wireless unit in communications with an access point, comprising:

transmitting a challenge text from the access point to the wireless unit;

receiving an encrypted challenge text and an initialization vector from the wireless unit, the initialization vector falling within a first group of initialization vectors, the first group including a plurality of initialization vectors solely used in connection with an authentication sequence; and

decrypting the encrypted challenge text using both the initialization vector and a pre-stored copy of a shared secret key to recover a challenge text.

15. (original) The method of claim 14, wherein the challenge text is a first sequence of bits.

16. (original) The method of claim 15, wherein the initialization vector is a second sequence of bits produced by a number generator.

17. (original) The method of claim 16, wherein the number generator is a pseudo-random number generator.

18. (original) The method of claim 14, wherein prior to transmitting the challenge text, the method further comprises negotiating the shared secret key between the access point and the wireless unit.

19. (original) The method of claim 14, wherein the decrypting of the encrypted challenge text includes

combining the initialization vector with the shared secret key; and

using a combination of the initialization vector and the shared secret key as a key material loaded to decrypt the encrypted challenge text.

20-23. (canceled)

24. (previously presented) An electronic device comprising:

a memory to contain a plurality of keys including a shared secret key;

a number generator;

a device management logic in communication with the memory and the number generator, the device management logic including

logic configured to analyze an initialization vector generated from the number generator to determine whether the initialization vector is used for either authentication or data communications; and

a wireless transceiver to transmit and receive information ~~for~~ configured to support the authentication.

25. (original) The electronic device of claim 24, wherein the authentication is Wired Equivalent Privacy (WEP) authentication.

26. (original) The electronic device of claim 24 is an access point.

27. (previously presented) An electronic device comprising:

means for generating an initialization vector;

means for determining whether the initialization vector falls within a first group of initialization vectors, the first group including a plurality of initialization vectors solely used in connection with an authentication sequence; and

means for encrypting information using the initialization vector for return to a source for the information using in part the initialization vector if the initialization vector falls within the first group.

28. (canceled)

29. (previously presented) The authentication method of claim 1, wherein the determining whether

the initialization vector falls within the first group includes determining whether the initialization vector forms numeric values within a range.

30. (previously presented) The authentication method of claim 9, wherein the selected series of bits is discontinuous.

31. (previously presented) The method of claim 14 wherein the plurality of initialization vectors of the first group form numeric values within a range.

32. (previously presented) The method of claim 14, the plurality of initialization vectors of the first group forms a continuous series of bits.

33. (previously presented) The method of claim 14, the plurality of initialization vectors of the first group forms a discontinuous series of bits.

34. (new) An authentication method comprising:

determining whether an initialization vector falls within a first group of initialization vectors, the first group including a plurality of initialization vectors solely used for authentication of a first electronic device; and

encrypting information using in part the initialization vector for return to the first electronic device if the initialization vector falls within the first group.

35. (new) The authentication method of claim 34, wherein the first electronic device is an access point.

36. (new) The authentication method of claim 34, wherein the determining whether the initialization vector falls within the first group includes determining whether a selected series of bits of the initialization vector has been set.

37. (new) The authentication method of claim 36, wherein the selected series of bits is continuous.

38. (new) The authentication method of claim 34 being conducted within a second electronic device and, wherein the encrypting of the information includes

combining the initialization vector with a shared secret key used by the first electronic device and the second electronic device; and

repeatedly performing bitwise Exclusive-OR (XOR) operations on the challenge text using a combination of the initialization vector with the shared secret key.